English Translation of Relevant Portions of JP-A-H11-298470
Published on October 29, 1999

:

:

Page (4), column 6, line 39 – Page (5), column 7, line 8

[0006] According to the present invention, a key manager divides a secret key S into a plurality of pieces of secret data S1 to Sn, loads at least one of the divided pieces of secret data Si on a storage medium (including one having a calculation function such as an IC card), and delivers the storage medium to a key user off-line. As to the rest of the divided pieces of secret data, they are sent to said key user on-line only when said key user is authenticated based on authentication data AS generated based on the secret data Si and identification data ID given to said key user.

[0007] In this way, even if the storage medium distributed off-line is stolen by an unauthorized person, it does not mean that the unauthorized person has obtained all the pieces of secret data S1 to Sn that are indispensable to decrypt the secret key S. Likewise, even if the secret data sent on-line is stolen by an unauthorized person, it does not mean that the unauthorized person has obtained all the pieces of secret data S1 to Sn that are indispensable to decrypt the secret key S. This makes it possible to reduce the possibility of secret key data being stolen while it is being distributed, and thus to improve the security of encrypted communication.

:

:

Page (7), column 11, lines 27–32

[0050] When the key user is authenticated by the above described authentication process, the encrypting/decrypting section 103 in the key manager device 100 encrypts the secret data S2 using the secret data S1 as a key. The communication section 107 in the key manager device 100 sends the encrypted secret data S2 to the key user device 200 via the communication line 400.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-298470
(43)Date of publication of application : 29.10.1999

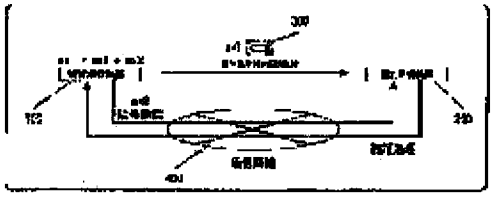
(51)Int.Cl. H04L 9/08
H04L 9/10
H04L 9/32

(21)Application number : 10-106437
(22)Date of filing : 16.04.1998

(71)Applicant : HITACHI LTD
(72)Inventor : YAMAZAKI MASANORI
NISHIOKA GENJI

(54) KEY DISTRIBUTION METHOD AND SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To reduce the possibility of being arrogated by an illegal person when distributing the secret key information to key users.
SOLUTION: A key manager device 100 divides a secret key S into secret information sets S1, S2, stores the information S1 to a storage medium 300 and distributes the information S1 to key users in off-line. A key user device 200 uses the secret information S1 having been stored in a distributed storage medium and identification information ID provided in advance for key users to make authentication processing with the key manager device 100. When the key user device 200 is authenticated, the key manager device 100 sends the remaining secret information S2 through a communication line 400 in on-line. The key user device 200 decodes the secret key S1 based on the secret information distributed in off-line and the secret key S2 sent in on-line.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－298470

(43)公開日　平成11年(1999)10月29日

(51)Int.Cl.[6]		識別記号	ＦＩ		
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ｅ
	9/10				６０１Ｂ
	9/32				６０１Ａ
					６２１Ａ
					６７５Ｄ

審査請求　未請求　請求項の数14　ＯＬ　（全９頁）

(21)出願番号　特願平10－106437

(22)出願日　平成10年(1998)４月16日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　山▲崎▼　正憲
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

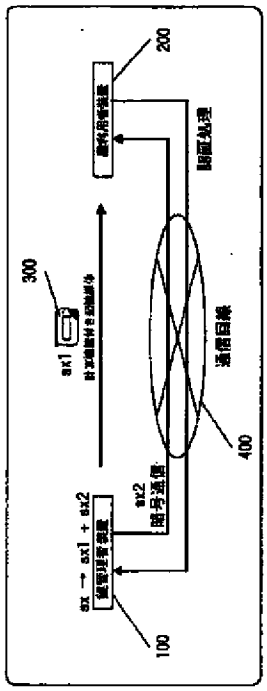
(72)発明者　西岡　玄次
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　富田　和子

(54)【発明の名称】　鍵の配布方法およびシステム

(57)【要約】
【課題】鍵管理者が鍵利用者に秘密鍵情報を配布する際、当該秘密鍵情報が不正者に横取りされる可能性を減少させる。
【解決手段】鍵管理者装置１００は、秘密鍵Ｓを秘密情報Ｓ１、Ｓ２に分割し、Ｓ１を記憶媒体３００に格納して鍵利用者にオフラインで配布する。鍵利用者装置２００は、配布された記憶媒体に格納されている秘密情報Ｓ１と予め鍵利用者に付与された識別情報ＩＤとを用いて、鍵管理者装置１００との間で認証処理を行う。認証された場合、鍵管理者装置１００は、残りの秘密情報Ｓ２を、通信回線４００を介して、オンライン送信する。鍵利用者装置２００は、オフライン配布された秘密情報Ｓ１とオンライン送信された秘密情報Ｓ２とを基に秘密鍵Ｓを復元する。

図1



1

【特許請求の範囲】

【請求項１】暗号通信に用いる鍵の配布方法であって、

鍵管理者の装置において、

秘密鍵Ｓを作成し、当該秘密鍵Ｓを少なくとも２つの秘密情報Ｓ１～Ｓｎ（ｎ≧２）に分割する第１のステップと、

前記第１のステップで得た秘密情報Ｓ１～Ｓｎのうちの少なくとも１つの秘密情報Ｓｉ（１≦ｉ≦ｎ）をオフラインで鍵利用者に配布する第２のステップと、

鍵利用者の装置において、

前記第２のステップによりオフラインで配布された秘密情報Ｓｉと、鍵管理者により予め付与された識別情報ＩＤとを基に、認証情報ＡＳを作成し、当該認証情報ＡＳを鍵管理者の装置に送信する第３のステップと、

鍵管理者の装置において、

前記第３のステップにより送信された認証情報ＡＳに基づいて、鍵利用者の認証処理を行う第４のステップと、

前記第４のステップにて鍵利用者が認証された場合、当該鍵利用者の装置に、前記第１のステップで得た秘密情報Ｓ１～Ｓｎのうち、前記第２のステップで当該鍵利用者にオフラインで配布した秘密情報Ｓｉ以外の秘密情報を送信する第５のステップと、

鍵利用者の装置において、

前記第５のステップにより送信された、秘密情報Ｓｉ以外の秘密情報Ｓ１～Ｓｎと、前記第２のステップによりオフラインで配布された秘密情報Ｓｉとを基に、前記秘密鍵Ｓを作成する第６のステップと、を備えることを特徴とする鍵の配布方法。

【請求項２】請求項１記載の鍵の配布方法であって、

前記第５のステップは、前記第４のステップにて鍵利用者が認証された場合、当該鍵利用者の装置に、前記第１のステップで得た秘密情報Ｓ１～Ｓｎのうち、前記第２のステップで当該鍵利用者にオフラインで配布した秘密情報Ｓｉ以外の秘密情報を、前記秘密情報Ｓｉを鍵として暗号化して送信するものであり、

前記第６のステップは、前記第５のステップにより送信された、秘密情報Ｓｉ以外の暗号化された秘密情報Ｓ１～Ｓｎを、前記秘密情報Ｓｉを鍵として復号化し、復号結果と前記秘密情報Ｓｉとを基に、前記秘密鍵Ｓを作成するものであることを特徴とする鍵の配布方法。

【請求項３】請求項１または２記載の鍵の配布方法であって、

鍵利用者の装置において、

前記第６のステップにより復元された秘密鍵Ｓを基に、認証情報ＡＳ´を作成し、当該認証情報ＡＳ´を鍵管理者の装置に送信する第７のステップと、

鍵管理者の装置において、

前記第７のステップにより送信された認証情報ＡＳ´に基づいて、鍵利用者の認証処理を行う第８のステップと、

2

鍵管理者の装置および／または鍵利用者の装置において前記第８のステップにて鍵利用者が認証された場合に、当該鍵利用者の、前記秘密鍵Ｓを用いた暗号通信に対する登録料金の課金処理を行う第９のステップを、さらに備えることを特徴とする鍵の配布方法。

【請求項４】鍵を生成する鍵管理者装置と、当該鍵管理者装置が生成した鍵を用いて暗号通信を行う鍵利用者装置と、でなる鍵の配布システムであって、

前記鍵管理者装置は、

秘密鍵Ｓを作成し、当該秘密鍵Ｓを少なくとも２つの秘密情報Ｓ１～Ｓｎ（ｎ≧２）に分割する鍵生成手段と、

前記鍵生成手段で得た秘密情報Ｓ１～Ｓｎのうちの少なくとも１つの秘密情報Ｓｉ（１≦ｉ≦ｎ）を記憶媒体に記憶する記憶手段と、

前記鍵利用者装置から送信された認証情報ＡＳを受信する第１の受信手段と、

前記受信手段で受信した認証情報ＡＳに基づいて、鍵利用者の認証処理を行う認証手段と、

前記認証手段により鍵利用者が認証された場合、前記鍵利用者装置に、前記鍵生成手段で得た秘密情報Ｓ１～Ｓｎのうち、前記記憶手段で記憶媒体に記憶した秘密情報Ｓｉ以外の秘密情報を送信する第１の送信手段と、を備え、

前記鍵利用者装置は、

前記鍵管理者装置により秘密情報Ｓｉが記憶された記憶媒体から、前記秘密情報Ｓｉを読み出す読出手段と、

前記読出手段により読み出された秘密情報Ｓｉと、鍵管理者により予め付与された識別情報ＩＤとを基に、認証情報ＡＳを作成する認証情報作成手段と、

前記認証情報作成手段により作成された認証情報ＡＳを前記鍵管理者装置に送信する第２の送信手段と、

前記鍵管理者装置により送信された、秘密情報Ｓｉ以外の秘密情報Ｓ１～Ｓｎを受信する第２の受信手段と、

前記読出手段により読み出された秘密情報Ｓｉと、前記第２の受信手段で受信した、秘密情報Ｓｉ以外の秘密情報Ｓ１～Ｓｎとを基に、前記鍵管理装置が生成した秘密鍵Ｓを復元する鍵復元手段と、を備えることを特徴とする鍵の配布システム。

【請求項５】鍵を生成する鍵管理者装置と、当該鍵管理者装置が生成した鍵を用いて暗号通信を行う鍵利用者装置と、計算機能付き記憶媒体と、でなる鍵の配布システムであって、

前記鍵管理者装置は、

秘密鍵Ｓを作成し、当該秘密鍵Ｓを少なくとも２つの秘密情報Ｓ１～Ｓｎ（ｎ≧２）に分割する鍵生成手段と、

前記鍵生成手段で得た秘密情報Ｓ１～Ｓｎのうちの少なくとも１つの秘密情報Ｓｉ（１≦ｉ≦ｎ）を、前記計算機能付き記憶媒体に記憶する記憶手段と、

前記鍵利用者装置から送信された認証情報ＡＳを受信する第１の受信手段と、

前記受信手段で受信した認証情報ＡＳに基づいて、鍵利用者の認証処理を行う認証手段と、

前記認証手段により鍵利用者が認証された場合、前記鍵利用者装置に、前記鍵生成手段で得た秘密情報Ｓ１～Ｓｎのうち、前記記憶手段で前記計算機能付き記憶媒体に記憶した秘密情報Ｓｉ以外の秘密情報を送信する第１の送信手段と、を備え、

前記鍵利用者装置は、

前記計算機能付き記憶媒体を接続する接続手段と、

前記接続手段により接続された前記計算機能付き記憶媒体から出力された認証情報ＡＳを前記鍵管理者装置に送信する第２の送信手段と、

前記鍵管理者装置から送信された、秘密情報Ｓｉ以外の秘密情報Ｓ１～Ｓｎを受信して、前記接続手段により接続された前記計算機能付き記憶媒体に出力する第２の受信手段と、を備え、

前記計算機能付き記憶媒体は、

記憶している秘密情報Ｓｉと鍵管理者により予め付与された識別情報ＩＤとをを基に、認証情報ＡＳを作成し、自己が接続している前記鍵利用者装置に出力する認証情報作成手段と、

記憶している秘密情報Ｓｉと、自己が接続している前記鍵利用者装置から出力された、秘密情報Ｓｉ以外の秘密情報Ｓ１～Ｓｎとを基に、前記鍵管理装置が生成した秘密鍵Ｓを復元する鍵復元手段と、を備えることを特徴とする鍵の配布システム。

【請求項６】暗号通信を行う鍵利用者に鍵を配布する情報処理装置であって、

秘密鍵Ｓを作成し、当該秘密鍵Ｓを少なくとも２つの秘密情報Ｓ１～Ｓｎ（ｎ≧２）に分割する鍵生成手段と、

前記鍵生成手段で得た秘密情報Ｓ１～Ｓｎのうちの少なくとも１つの秘密情報Ｓｉ（１≦ｉ≦ｎ）を記憶媒体に記憶する記憶手段と、

鍵利用者の装置から送信された、秘密情報Ｓｉと当該鍵利用者に予め付与した識別情報とを基に作成された認証情報ＡＳを受信する受信手段と、

前記受信手段で受信した認証情報ＡＳに基づいて、鍵利用者の認証処理を行う認証手段と、

前記認証手段により鍵利用者が認証された場合、当該鍵利用者の装置に、前記鍵生成手段で得た秘密情報Ｓ１～Ｓｎのうち、前記記憶手段で記憶媒体に記憶した秘密情報Ｓｉ以外の秘密情報を送信する送信手段と、を備えることを特徴とする情報処理装置。

【請求項７】請求項６記載の情報処理装置であって、

前記認証手段により鍵利用者が認証された場合、前記鍵生成手段で得た秘密情報Ｓ１～Ｓｎのうち、前記記憶手段で記憶媒体に記憶した秘密情報Ｓｉ以外の秘密情報を、前記秘密情報Ｓｉを鍵として暗号化し、前記送信手段に出力する暗号化手段をさらに備えることを特徴とする情報処理装置。

【請求項８】請求項６または７記載の情報処理装置であって、

前記受信手段は、鍵利用者の装置から送信された、秘密鍵Ｓを基に作成された認証情報ＡＳ´を受信するものであり、

前記認証手段は、前記受信手段で受信した認証情報ＡＳ´に基づいて、鍵利用者の認証処理を行うものであり、

前記認証手段により、認証情報ＡＳ´に基づいて鍵利用者が認証された場合に、当該鍵利用者の、前記秘密鍵Ｓを用いた暗号通信に対する登録料金を特定する情報を記憶する課金手段を、さらに備えることを特徴とする情報処理装置。

【請求項９】鍵管理者の装置にて、秘密鍵Ｓを少なくとも２つに分割することで得られた秘密情報Ｓ１～Ｓｎ（ｎ≧２）を基に鍵を復元する情報処理装置であって、

鍵管理者から配布された記憶媒体に記憶された秘密情報Ｓｉ（１≦ｉ≦ｎ)を読み出す読出手段と、

前記読出手段により読み出された秘密情報Ｓｉと、鍵管理者により予め付与された識別情報ＩＤとを基に、認証情報ＡＳを作成する認証情報作成手段と、

前記認証情報作成手段により作成された認証情報ＡＳを鍵管理者の装置に送信する送信手段と、

鍵管理者の装置から送信された、秘密情報Ｓｉ以外の秘密情報Ｓ１～Ｓｎを受信する受信手段と、

前記読出手段により読み出された秘密情報Ｓｉと、前記受信手段で受信した、秘密情報Ｓｉ以外の秘密情報Ｓ１～Ｓｎとを基に、秘密鍵Ｓを復元する鍵復元手段と、を備えることを特徴とする情報処理装置。

【請求項１０】請求項９記載の情報処理装置であって、

鍵管理者の装置から送信された、秘密情報Ｓｉ以外の秘密情報Ｓ１～Ｓｎは、秘密情報Ｓｉを鍵として暗号化されたものであり、

前記受信手段で受信した、秘密情報Ｓｉ以外の暗号化された秘密情報Ｓ１～Ｓｎを、前記読出手段により読み出された秘密情報Ｓｉを鍵として復号化し、前記鍵復元手段に出力する復号化手段をさらに備えることを特徴とする情報処理装置。

【請求項１１】請求項９または１０記載の情報処理装置であって、

前記認証情報作成手段は、前記鍵復元手段により復元された秘密鍵Ｓを基に、認証情報ＡＳ´を作成するものであり、

前記送信手段は、前記認証情報作成手段により作成された認証情報ＡＳ´を鍵管理者の装置に送信するものであり、

鍵管理者の装置にて、前記認証情報ＡＳ´により鍵利用者が認証された場合に、当該鍵利用者の、前記秘密鍵Ｓを用いた暗号通信に対する登録料金を特定する情報を記憶する課金手段を、さらに備えることを特徴とする情報処理装置。

5

【請求項１２】鍵管理者の装置にて、秘密鍵Ｓを少なくとも２つに分割することで得られた秘密情報Ｓ１～Ｓｎ（ｎ≧２）を基に鍵を復元する、当該鍵を用いて暗号通信を行う鍵利用者の装置に挿抜可能に構成された計算機能付き記憶媒体であって、
記憶している秘密情報Ｓｉ（１≦ｉ≦ｎ）と、鍵管理者により予め付与された識別情報ＩＤとを基に認証情報ＡＳを作成し、自己が接続している鍵利用者の装置を介して、鍵管理者の装置に送信する認証情報作成手段と、
鍵管理者の装置により記憶された秘密情報Ｓｉと、自己が接続している鍵利用者の装置を介して受け取った、鍵管理者の装置が送信した秘密情報Ｓｉ以外の秘密情報Ｓ１～Ｓｎとを基に、前記秘密鍵Ｓを復元する鍵復元手段と、を備えることを特徴とする計算機能付き記憶媒体。
【請求項１３】請求項１２記載の計算機能付き記憶媒体であって、
鍵管理者の装置から送信された、秘密情報Ｓｉ以外の秘密情報Ｓ１～Ｓｎは、秘密情報Ｓｉを鍵として暗号化されたものであり、
自己が接続している前記鍵利用者装置が受信した、秘密情報Ｓｉ以外の暗号化された秘密情報Ｓ１～Ｓｎを、記憶している秘密情報Ｓｉを鍵として復号化し、前記鍵復元手段に出力する復号化手段をさらに備えることを特徴とする計算機能付き記憶媒体。
【請求項１４】請求項１２または１３記載の計算機能付き記憶媒体であって、
前記認証情報作成手段は、前記鍵復元手段により復元された秘密鍵Ｓを基に、認証情報ＡＳ´を作成し、自己が接続している鍵利用者の装置を介して、鍵管理者の装置に送信するものであり、
鍵管理者の装置にて、前記認証情報ＡＳ´により鍵利用者が認証された場合に、当該鍵利用者の、前記秘密鍵Ｓを用いた暗号通信に対する登録料金を特定する情報を記憶する課金手段を、さらに備えることを特徴とする計算機能付き記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する分野】本発明は、暗号通信に用いる鍵を鍵利用者（たとえば、暗号データの受信者）に配布する技術に関する。
【０００２】
【従来の技術】一般に、大量のデータを暗号通信する場合、秘密鍵暗号が用いられている。秘密鍵暗号では、送信者と受信者との間で共通の鍵（共通鍵）を持つ必要がある。共通鍵の配送方法としては、コピー鍵方式、個別鍵方式等があるが、いずれの場合においても、秘密鍵情報を受信者に配布しなければならない。従来は、たとえば、ＩＣカード等に秘密鍵情報を搭載して、受信者にオフラインで配布したり、あるいは、暗号通信等により受信者に秘密鍵情報を送信することで、秘密鍵情報を受信者に配布している。

6

【０００３】
【発明が解決しようとする課題】しかしながら、秘密鍵情報をＩＣカード等に搭載してオフラインで配布する方法では、不正者がこの記憶媒体を盗用し、正規の受信者になりすます可能性が考えられる。また、秘密鍵情報を暗号通信等により送信する方法では、不正者が秘密鍵情報を盗聴・解読し、正規の受信者になりすます可能性が考えられる。
【０００４】本発明は、上記事情に鑑みてなされたものであり、本発明の目的は、秘密鍵情報を配布する際に、当該秘密鍵情報が不正者に横取りされる可能性を減少させ、暗号通信のセキュリティを向上させることにある。
【０００５】
【課題を解決するための手段】上記課題を解決するために、本発明は、暗号通信に用いる鍵の配布方法であって、鍵管理者の装置において、秘密鍵Ｓを作成し、当該秘密鍵Ｓを少なくとも２つの秘密情報Ｓ１～Ｓｎ（ｎ≧２）に分割する第１のステップと、前記第１のステップで得た秘密情報Ｓ１～Ｓｎのうちの少なくとも１つの秘密情報Ｓｉ（１≦ｉ≦ｎ）をオフラインで鍵利用者に配布する第２のステップと、鍵利用者の装置において、前記第２のステップによりオフラインで配布された秘密情報Ｓｉと、鍵管理者により予め付与された識別情報ＩＤとを基に、認証情報ＡＳを作成し、当該認証情報ＡＳを鍵管理者の装置に送信する第３のステップと、鍵管理者の装置において、前記第３のステップにより送信された認証情報ＡＳに基づいて、鍵利用者の認証処理を行う第４のステップと、前記第４のステップにて鍵利用者が認証された場合、当該鍵利用者の装置に、前記第１のステップで得た秘密情報Ｓ１～Ｓｎのうち、前記第２のステップで当該鍵利用者にオフラインで配布した秘密情報Ｓｉ以外の秘密情報を送信する第５のステップと、鍵利用者の装置において、前記第５のステップにより送信された、秘密情報Ｓｉ以外の秘密情報Ｓ１～Ｓｎと、前記第２のステップによりオフラインで配布された秘密情報Ｓｉとを基に、前記秘密鍵Ｓを作成する第６のステップと、を備えることを特徴とする。
【０００６】本発明によれば、鍵管理者は、秘密鍵Ｓを複数の秘密情報Ｓ１～Ｓｎに分割し、そのうちの少なくとも１つの秘密情報Ｓｉを記憶媒体（ＩＣカード等の計算機能付き記憶媒体を含む）に搭載してオフラインで鍵利用者に配布している。そして、残りについては、秘密情報Ｓｉおよび鍵利用者に付与された識別情報ＩＤを基に作成した認証情報ＡＳにより鍵利用者を認証した場合にのみ、当該鍵利用者にオンラインで送信するようにしている。
【０００７】このようにすることで、たとえ、オフラインで配布した記憶媒体が不正者に盗用されたとしても、それだけでは、不正者は、秘密鍵Ｓを復元するのに必要

なすべての秘密情報Ｓ１～Ｓｎを取得したことにならない。同様に、オンラインで送信した秘密情報が不正者に盗聴されたとしても、それだけでは、不正者は、秘密鍵Ｓを復元するのに必要なすべての秘密情報Ｓ１～Ｓｎを取得したことにならない。このため、秘密鍵情報を配布する際に、当該秘密鍵情報が不正者に横取りされる可能性を減少させることができ、ひいては、暗号通信のセキュリティを向上させることができる。

【０００８】なお、本発明において、第５のステップは、第４のステップにて鍵利用者が認証された場合、当該鍵利用者の装置に、前記第１のステップで得た秘密情報Ｓ１～Ｓｎのうち、前記第２のステップで当該鍵利用者にオフラインで配布した秘密情報Ｓｉ以外の秘密情報を、前記秘密情報Ｓｉを鍵として暗号化して送信するものであり、第６のステップは、第５のステップにより送信された、秘密情報Ｓｉ以外の暗号化された秘密情報Ｓ１～Ｓｎを、前記秘密情報Ｓｉを鍵として復号化し、復号結果と前記秘密情報Ｓｉとを基に、前記秘密鍵Ｓを作成するものでもよい。

【０００９】このようにすることで、秘密情報Ｓｉ以外の秘密情報Ｓ１～Ｓｎをオンラインで送信する際のセキュリティをさらに向上させることができる。

【００１０】

【発明の実施の形態】以下に、本発明の一実施形態について説明する。

【００１１】図１は、本発明の一実施形態である秘密鍵配布方法が適用されたシステムの概略図である。

【００１２】図示するように、本実施形態方法は、相互に通信回線400で接続された鍵管理者装置１００および鍵利用者装置２００と、鍵管理者装置１００および鍵利用者装置２００に挿抜可能に構成された計算機能付き記憶媒体３００と、を含んで構成されるシステムにおいて実施される。

【００１３】図２に、鍵管理者装置１００の概略機能構成を示す。

【００１４】図示するように、鍵管理者装置１００は、乱数生成部１０１と、演算部１０２と、暗復号化部１０３と、認証部１０４と、課金部１０５と、メモリ１０６と、通信部１０７と、で構成される。これらの機能構成は、コンピュータにおいて、各機能を実現するための手順が記述されたプログラムを実行することにより、ソフトウエア的に実現されるものでもよいし、あるいは、各機能を実現するロジックを組むことによりハードウエア的に実現されるようにしてもよい。ソフトウエア的に実現される場合は、各機能を実現するための手順が記述されたプログラムを、ＣＤ－ＲＯＭ等の記憶媒体に格納して、コンピュータに供給するようにしてもよい。

【００１５】なお、鍵管理者装置１００には、オフラインで鍵利用者に配布する計算機能付き記憶媒体３００を接続するための機構が設けられている。

【００１６】図３に、鍵利用者装置２００の概略機能構成を示す。

【００１７】図示するように、鍵利用者装置２００は、乱数生成部２０１と、素数生成部２０２と、演算部２０３と、暗復号化部２０４と、メモリ２０５と、通信部２０６と、で構成される。これらの機能構成は、鍵管理者装置１００と同様、コンピュータにおいて、各機能を実現するため手順が記述されたプログラムを実行することにより、ソフトウエア的に実現されるものでもよいし、あるいは、各機能を実現するロジックを組むことによりハードウエア的に実現されるようにしてもよい。ソフトウエア的に実現される場合は、各機能を実現するための手順が記述されたプログラムを、ＣＤ－ＲＯＭ等の記憶媒体に格納して、コンピュータに供給するようにしてもよい。

【００１８】なお、鍵利用者装置２００は、オフラインで鍵管理者から配布された計算機能付き記憶媒体３００を接続するための機構が設けられている。

【００１９】図４に、計算機能付き記憶媒体３００の概略機能構成を示す。

【００２０】図示するように、計算機能付き記憶媒体３００は、暗復号化部３０１と、演算部３０２と、メモリ３０３と、で構成される。これらの機能構成は、ＩＣカードにおいて、各機能を実現するため手順が記述されたプログラムを実行することにより、ソフトウエア的に実現されるものでもよいし、あるいは、各機能を実現するロジックを組むことによりハードウエア的に実現されるようにしてもよい。

【００２１】次に、上記説明したシステムにおいて実施される、本発明の第一実施形態である秘密鍵配布方法について説明する。

【００２２】まず、鍵管理者装置１００は、鍵管理者の指示にしたがい、乱数生成部１０１によって、乱数Ｓを生成し、これを鍵利用者の秘密鍵とする。その後、演算部１０２により秘密鍵Ｓを秘密情報Ｓ１、Ｓ２に分割し、秘密鍵Ｓ、および秘密情報Ｓ１、Ｓ２をメモリ１０６に格納する。次に、鍵管理者装置１００は、メモリ１０６から秘密情報Ｓ１を取り出し、これを鍵管理者装置１００に接続された計算機能付き記憶媒体３００内のメモリ３０３に格納する。

【００２３】鍵管理者は、秘密情報Ｓ１が格納された計算機能付き記憶媒体３００を対象となる鍵利用者にオフラインで配布する。

【００２４】秘密情報Ｓ１が格納された計算機能付き記憶媒体３００を受け取った鍵利用者は、これを鍵利用者装置２００に接続する。

【００２５】鍵利用者装置２００は、鍵利用者の指示にしたがい、計算機能付き記憶媒体３００から秘密情報Ｓ１を取り出し、秘密情報Ｓ１と鍵管理者により予め付与された当該鍵利用者の識別情報ＩＤとを使って、鍵管理

者装置１００との間で認証処理を行う。

【００２６】認証処理には様々な方法があるが、ここでは、一例として、ＲＳＡ署名法を用いた場合とエルガマル署名法を用いた場合とについて、説明する。

【００２７】まず、ＲＳＡ署名法を用いた場合について説明する。

＊

数1

・秘密情報　　p,q：素数

・署名鍵　　(d,n), $d \in \mathbb{Z}$, $n=pq$

・検証鍵　　(e,n), $e \in \mathbb{Z}$, $n=pq$　　･･･(数1)

【００３０】ここで、署名鍵は秘密、検証鍵は公開とする。鍵利用者装置２００は、署名鍵と、鍵利用者が入力した、鍵管理者により予め付与された当該鍵利用者の識別情報ＩＤとを計算機能付き記憶媒体３００に出力する。これを受けて、計算機能付き記憶媒体３００は、演算部３０２により、

【００３１】

【数2】

数2

$$AS = S'^{d} \pmod{n} \qquad \cdots(数2)$$

【００３２】から認証情報ＡＳを計算する。ここで、Ｓ´は、秘密情報Ｓ１と識別情報ＩＤとを入力とする所定の関数の値（たとえば、ハッシュ値）である。次に、計算機能付き記憶媒体３００は、認証情報ＡＳを鍵利用者装置２００に出力する。これを受けて、鍵利用者装置２００は、通信部２０６により、認証情報ＡＳを、通信回線４００を介して、鍵管理者装置１００に送信する。

【００３３】鍵管理者装置１００は、通信部１０７により認証情報ＡＳを受信すると、認証部１０４により、

【００３４】

【数3】

数3

$$S' = AS^{e} \pmod{n} \qquad \cdots(数3)$$

【００３５】が成立するか否かを検証し、成立すれば、認証情報ＡＳを送ってきた鍵利用者装置２００の鍵利用者が正当な鍵利用者であると認証する。なお、鍵管理者装置１００は、鍵利用者に付与した識別情報ＩＤを、当該鍵利用者にオフラインで配布した計算機能付き記憶媒体３００に格納された秘密情報Ｓ１と対応付けて、メモリ１０６に格納しているものとする。

【００３６】次に、エルガマル署名法を用いた場合について説明する。

【００３７】鍵利用者装置２００は、鍵利用者の指示にしたがい、素数生成部２０２により素数ｐを生成し、演算部２０２により、

【００３８】

【数4】

数4

$$\mathrm{ord}_{p}(\alpha)=p-1 \qquad \cdots(数4)$$

【００３９】を満たすαを作成する。そして、作成したαおよび素数ｐを計算機能付き記憶媒体３００に出力する。これを受けて、計算機能付き記憶媒体３００は、演算部３０２により、

【００４０】

【数5】

数5

$$y = \alpha^{s'} \pmod{p} \qquad \cdots(数5)$$

【００４１】を満たすｙを計算し、署名鍵を（ｘ，α，ｐ）、検証鍵を（ｙ，α，ｐ）とする。ここで、Ｓ´は、秘密情報Ｓ１と識別情報ＩＤとを入力とする所定の関数の値（たとえば、ハッシュ値）である。

【００４２】次に、鍵利用者装置２００は、ｐ－１と互いに素な乱数ｋを乱数生成部２０１により作成し、

【００４３】

【数6】

数6

$$r = a^{k} \pmod{p} \qquad \cdots(数6)$$

【００４４】を満たすｒを計算する。さらに、適当なメッセージｍを乱数生成部２０１により生成し、ｒ、ｋとともに計算機能付き記憶媒体３００に出力する。これを受けて、計算機能付き記憶媒体３００は、演算部３０２により、

【００４５】

【数7】

数7

$$t = (m - S'r)k^{-1} \pmod{p-1} \qquad \cdots(数7)$$

【００４６】を満たすｔを計算する。そして、（ｒ，ｔ）をメッセージｍに対する署名とし、メッセージｍ，署名（ｒ，ｓ）を、鍵利用者装置２００に出力する。これを受けて、鍵利用者装置２００は、通信部２０６より、メッセージｍ，署名（ｒ，ｓ）を、通信回線４００を介して、鍵管理者装置１００に送信する。

【００４７】鍵管理者装置１００は、メッセージｍ，署名（ｒ，ｓ）を受け取ると、認証部１０４により、

【００４８】

【数８】

数8

$$\alpha^m = y^r r^t \pmod{p} \qquad \cdots(数8)$$

【００４９】が成立するか否かを検証し、成立すれば、メッセージｍ，署名（ｒ，ｓ）を送ってきた鍵利用者装置２００の鍵利用者が正当な鍵利用者であると認証する。なお、鍵管理者装置１００は、鍵利用者に付与した識別情報ＩＤを、当該鍵利用者にオフラインで配布した計算機能付き記憶媒体３００に格納された秘密情報Ｓ１と対応付けて、メモリ１０６に格納しているものとする。

【００５０】以上説明した認証処理により、鍵利用者が認証されると、鍵管理者装置１００は、暗復号化部１０３により、秘密情報Ｓ１を鍵として秘密情報Ｓ２を暗号化する。そして、通信部１０７により、暗号化された秘密情報Ｓ２を、通信回線４００を介して、鍵利用者装置２００に送信する。

【００５１】鍵利用者装置２００は、暗号化された秘密情報Ｓ２を受け取ると、これを計算機能付き記憶媒体３００に出力する。これを受けて、計算機能付き記憶媒体３００は、暗復号化部３０１により、暗号化された秘密情報Ｓ２を、秘密情報Ｓ１を鍵として復号化し、メモリ３０３に格納する。さらに、演算装置３０２により、復号化された秘密情報Ｓ２、および秘密情報Ｓ１を基に、秘密鍵Ｓを復元し、メモリ３０３に格納する。

【００５２】次に、鍵利用者装置２００は、鍵利用者の指示にしたがい、計算機能付き記憶媒体３００から秘密鍵Ｓを取り出し、この秘密鍵Ｓを使って、鍵管理者装置１００との間で、上記と同様の手順により認証処理を行う。

【００５３】なお、ＲＳＡ署名法を用いる場合は、上記の（数２）、（数３）において、Ｓ´の代わりに秘密鍵Ｓを用いればよい。また、エルガマル署名法を用いる場合には、上記の（数５）、（数７）において、Ｓ´の代わりに秘密鍵Ｓを用いればよい。

【００５４】鍵利用者が認証されると、鍵管理者装置１００は、課金部１０５により、当該鍵利用者の、秘密鍵Ｓを用いた暗号通信に対する登録料金情報（課金情報）を生成し、これをメモリ１０６に格納する。この情報は、当該鍵利用者への料金請求に際して利用される。

【００５５】上記の処理により、鍵利用者に秘密鍵Ｓが配布されると、鍵利用者は、秘密鍵Ｓを用いて、情報提供者との間で暗号通信を行う。あるいは、秘密鍵Ｓを用いて情報提供者との間で鍵共有を行った後に、その共有鍵により暗号通信を行う。

【００５６】ここで、鍵管理者と情報提供者とが同一である場合における、鍵利用者および情報提供者間で暗号通信を行うためのシステムを図５に示す。図示するように、情報提供者装置５００は、鍵管理者装置１００により鍵利用者に配布した秘密鍵Ｓを用いて、当該鍵利用者の鍵利用者装置２００との間で、暗号通信を行う。

【００５７】本実施形態では、鍵管理者は、秘密鍵Ｓを秘密情報Ｓ１、Ｓ２に分割し、秘密情報Ｓ１を記憶媒体（ＩＣカード等の計算機能付き記憶媒体を含む）に搭載してオフラインで鍵利用者に配布している。そして、秘密情報Ｓ２については、秘密情報Ｓ１および鍵利用者に付与された識別情報ＩＤを基に作成した認証情報ＡＳにより鍵利用者を認証した場合にのみ、当該鍵利用者にオンラインで送信するようにしている。

【００５８】このようにすることで、たとえ、オフラインで配布した記憶媒体が不正者に盗用されたとしても、それだけでは、不正者は、秘密鍵Ｓを復元するのに必要なすべての秘密情報Ｓ１、Ｓ２を取得することができない。このため、秘密鍵情報を配布する際に、当該秘密鍵情報が不正者に横取りされる可能性を減少させることができ、ひいては、暗号通信のセキュリティを向上させることができる。

【００５９】また、本実施形態において、鍵管理者装置１００は、秘密情報Ｓ１および鍵利用者に付与された識別情報ＩＤを基に作成した認証情報ＡＳにより鍵利用者が認証された場合、鍵利用者装置２００に、秘密情報Ｓ２を、秘密情報Ｓ１を鍵として暗号化して送信し、鍵利用者装置２００は、暗号化された秘密情報Ｓ２を、秘密情報Ｓ１を鍵として復号化し、復号結果と秘密情報Ｓ１とを基に、秘密鍵Ｓを復元している。このようにすることで、秘密情報Ｓ２をオンラインで送信する際のセキュリティをさらに向上させることができる。

【００６０】なお、上記の実施形態では、秘密鍵Ｓを２つの秘密情報Ｓ１、Ｓ２に分割する場合について説明した。しかしながら、本発明はこれに限定されるものではなく、秘密鍵Ｓを少なくとも２つの秘密情報Ｓ１～Ｓｎ

に分割するようにしてもよい。この場合、そのうちの少なくとも１つをオフラインで配布し、残りを通信回線を使って、オンラインで送信するようにすればよい。

【００６１】また、上記の実施形態では、鍵管理者装置１００の課金部１０５により、課金情報を鍵管理者装置１００内のメモリ１０６に格納するようにしたものについて説明したが、本発明はこれに限定されない。たとえば、課金部１０５を、鍵管理者装置１００に設ける代わりに、鍵利用者装置２００あるいは計算機能付き記憶媒体３００に設け、課金情報を鍵利用者装置２００内のメモリ２０５あるいは計算機能付き記憶媒体３００内のメモリ３０３に格納するようにしてもよい。この情報は、鍵利用者への料金請求に際し、鍵管理者装置１００に吸い上げられて利用される。

【００６２】

【発明の効果】以上説明したように、本発明によれば、鍵管理者が鍵利用者に秘密鍵情報を配布する際、当該秘密鍵情報が不正者に横取りされる可能性を減少させることができ、ひいては、暗号通信のセキュリティを向上させることができる。

【図面の簡単な説明】

【図１】本発明の一実施形態である秘密鍵配布方法が適用されたシステムの概略図である。

＊【図２】図１に示す鍵管理者装置１００の概略機能構成図である。

【図３】図１に示す鍵利用者装置２００の概略機能構成図である。

【図４】図１に示す計算機能付き記憶媒体３００の概略機能構成図である。

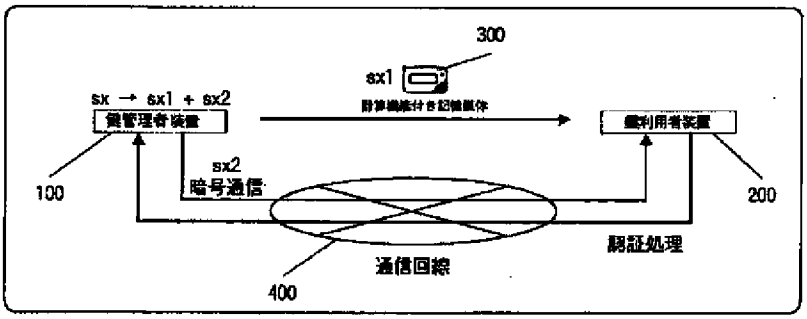
【図５】鍵管理者と情報提供者とが同一である場合における、鍵利用者および情報提供者間で暗号通信を行うためのシステムの概略図である。

【符号の説明】

１００　鍵管理者装置
１０１、２０１　乱数生成部
１０２、２０３、３０２　演算部
１０３、２０４、３０１　暗復号化部
１０４　認証部
１０５　課金部
１０６、２０５、３０３　メモリ
１０７、２０６　通信部
２００　鍵利用者装置
２０２　素数生成部
３００　計算機能付き記憶媒体
４００　通信回線
５００　情報提供者装置

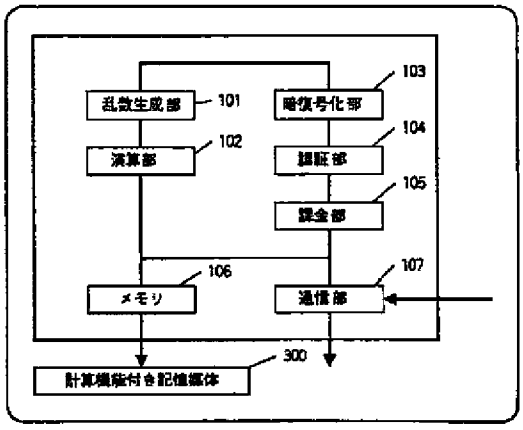
【図１】

図1



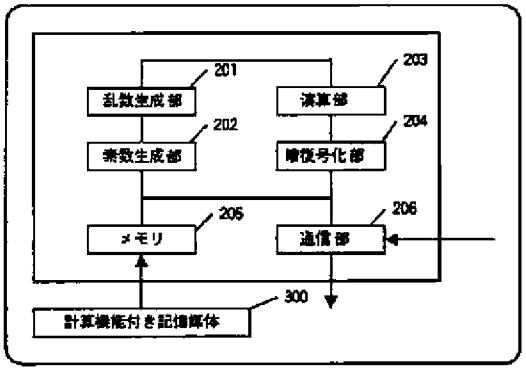
【図２】

図2



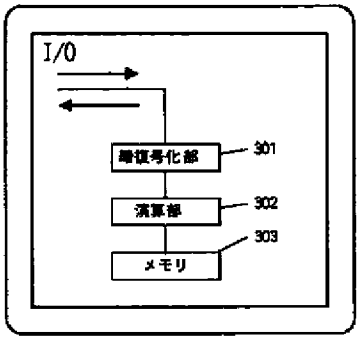
【図３】

図3



【図４】

図4



【図５】

図5